

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-3 and 5-10 are pending in this application, Claim 4 having been canceled without prejudice or disclaimer; and Claims 1, 5, and 8 having been presently amended. Support for amended Claims 1, 5, and 8 can be found, for example, in the original claims, drawings, and specification as originally filed.<sup>1</sup> No new matter has been added.

In the outstanding Office Action, Claims 1-3, 5, 6, and 8-10 were rejected under 35 U.S.C. § 103(a) as unpatentable over Ginter et al. (U.S. Patent No. 6,253,193; hereinafter “Ginter”) in view of Hughes (U.S. Patent No. 6,748,537); and Claims 4 and 7 were rejected under 35 U.S.C. § 103(a) as unpatentable over Ginter and Hughes in view of Matsuyama et al. (U.S. Patent Publication No. 2002/0026581; hereinafter “Matsuyama”).

In response to the rejections under 35 U.S.C. § 103(a), Applicants have amended Claim 1 to recite features formerly of Claim 4. Applicants respectfully submit that independent Claim 1 recites novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1 is directed to a computer-readable storage medium including, *inter alia*:

...a first execution file recorded on said computer-readable storage medium using a copy protection mechanism, said first execution file including

authenticating means for performing an authentication process with a second execution file,

key obtaining means for obtaining unique key information unique to said first execution file, and

transmitting means for transmitting said unique key information to said second execution file,

---

<sup>1</sup> See original Claim 4.

wherein said first execution file is executed by an information processing apparatus including a processor, when said computer-readable storage medium is inserted into said information processing apparatus and said second execution file generates a content key from said unique key information, decrypts encrypted content using the content key, and reproduces the decrypted content, and

***wherein said content is recorded on said computer-readable storage medium and said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said content, and said transmitting means transmits said content to said second execution file based on said digital signature information.***

Independent Claims 5 and 8 recite substantially similar features as independent Claim

1. Thus, the arguments presented below with respect to independent Claim 1 are also applicable to independent Claims 5 and 8.

Page 9 of the outstanding Office Action acknowledges that “Ginter and Hughes do not specifically disclose encrypting digital signature information attached to said content; and said transmitting means transmits said content to said second execution file based on said digital signature information.” In an attempt to cure the above-noted deficiencies of Ginter and Hughes, the outstanding Office Action cites paragraphs [0160]-[0169] of Matsuyama.

However, Applicants respectfully submit that Matsuyama fails to teach or suggest that “said content is recorded on said computer-readable storage medium and said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said content, and said transmitting means transmits said content to said second execution file based on said digital signature information,” as recited in Applicants’ independent Claim 1.

Paragraph [0163] of Matsuyama states:

The user A presents his/her public key to the certificate authority 202 and receives a public key certificate including a digital signature written by the certificate authority. After the service provider (SP) 203 authenticates the user A on the basis of the identification certificate (IDC), the service provider (SP)

203 extracts the public key from the public key certificate of the user A and transmits a content to the user A after encrypting the content using the extracted public key. When the user A of the user device A205 receives the encrypted content, the encrypted data is decrypted using a private key corresponding to the public key, and the decrypted data is used by the user A.

Thus, in Matsuyama, a service provider 203 extracts the public key from a public key certificate of the user A and transmits a content to the user A after encrypting the content using the extracted public key. However, Matsuyama does not describe that the content is transmitted to a second execution file based on the digital signature information. In Matsuyama, the service provider 203 transmits the content to a first user, not a second execution file. Also, Matsuyama's content is not transmitted based on digital signature information that is attached to the content.

Thus, Applicants respectfully submit that amended independent Claims 1, 5, and 8 (and all claims depending thereon) patentably distinguish over the cited references.

Accordingly, Applicants respectfully request the rejections under 35 U.S.C. §103(a) be withdrawn.

Consequently, in view of the present amendment, and in light of the above discussion, the pending claims as presented herewith are believed to be in condition for formal allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



---

Bradley D. Lytle  
Attorney of Record  
Registration No. 40,073

Derek P. Benke  
Registration No. 56,944

Customer Number  
**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/07)  
DPB/rac

I:\ATTY\DPB\27's\277771US\277771US-AM3.DOC